UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

BC8

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
08/994,878	12/19/97	EPSTEIN M	PHA-23.313

EXAMINER	
SONG, H	
ART UNIT	PAPER NUMBER
2131	13

DATE MAILED: 05/23/01

WM31/0523

JACK E HAKEN
US PHILIPS CORP
INTELLECTUAL PROP DEPT
580 WHITE PLAINS ROAD
TARRYTOWN NY 10591

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

Office Action Summary

Application No.	Applicant(s)
08/994,878	Epstein
Examiner	**Art Unit**
Ho S. Song	2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136 (a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on *Feb 23, 2001*.

2a) ☒ This action is **FINAL.** 2b) ☐ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11; 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above, claim(s) *3, 4, 9, 10, 17, and 18* is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) *1, 2, 5-8, 11-16, and 19* is/are rejected.

7) ☒ Claim(s) *20* is/are objected to.

8) ☐ Claims _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are objected to by the Examiner.

11) ☐ The proposed drawing correction filed on _____ is: a) ☐ approved b) ☐ disapproved.

12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

13) ☐ Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

a) ☐ All b) ☐ Some* c) ☐ None of:

1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

*See the attached detailed Office action for a list of the certified copies not received.

14) ☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

Attachment(s)

15) ☒ Notice of References Cited (PTO-892)
16) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
17) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s). _____
18) ☐ Interview Summary (PTO-413) Paper No(s). _____
19) ☐ Notice of Informal Patent Application (PTO-152)
20) ☐ Other:

DETAILED ACTION

Objections

1. Claim 20 is objected. Claim 20 is dependent on canceled claim 18.

Claim Rejections - 35 USC § 103

2 The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

3 Claim 5 is rejected under 35 U.S.C. 103(a) as being unpatentable by Trostle(US 5,919,257).

In claim 5, Trostle teaches user transmitting ID over the network in (col.5, lines 50-51). Trostle discloses reading from a storage data corresponding to the user having the received ID, which data comprises the user's private key encrypted using a key determined from identifying information of the user and sending via network the encrypted private key, whereby the encrypted key can be received and decrypted at the location of the user's identifying information in (col.5, lines 51-57). Trostle does not discloses destroying any non-volatile record of the private key at the location of the user. Trostle does discloses destroying a password at user's location in (col.6, lines 3-6). It would have been obvious to a person of ordinary skill in the art to modify the invention of Trostle to erase private key rather than erasing password alone because by completely deleting password as well as private key would greatly reduces chance of stealing valuable data by hackers thus providing a greater security..

4. Claims 6-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Trostle in view of Schneier.

In claim 6, Trostle discloses all the limitations above. However, Trostle does not discloses Passphrase scheme. Schneier discloses passphrase scheme in (page 174, passphrase section). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use passphrase taught in Schneier for password of Trostle so that user can remember phrases easier than random character sequences. Passphrase provides greater security through increased entropy than a short password

In claims, 7,8, Trostle discloses receiving a digital signature manifesting the user's approval of a document, which digital signature represents a computed hash of the approved document encrypted using the user's private key and verifying the received digital signature by decrypting the digital signature using the user's public key and comparing the result of this decrypting with an independently computed hash of the document in (fig.6, col.2, lines 44-60, col.6, lines 10-25).

5. Claims 1,11,13,15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Trostle in view of Spies (US 5,689,565)..

In claim 1, Trostle discloses user transmitting ID over the network in (col.5, lines 50-51). Trostle discloses reading from a storage data corresponding to the user having the received ID, which data comprises the user's private key encrypted using a key determined from identifying

information of the user and sending via network the encrypted private key, whereby the encrypted key can be received and decrypted at the location of the user's identifying information in (col.5, lines 51-57). However, Trostle does not specifically discloses public key corresponding to the private key. The examiner asserts that Trostle teaches asymmetric key system by user transmitting username over the network and remote server compares username against a list and transmits corresponding private key to the user. It would have been obvious to person of ordinary skill in the art to recognize that this is a public key system. One of ordinary skill in the art would be motivated to use public key scheme because it is faster and it provides better security than symmetric key system. Trostle does not teach encrypting or decrypting the hash value using the user's private key. Spies discloses this feature in (col.9, lines 15-30). It would have been obvious to person of ordinary skill in the art at the time the invention was made to encrypt hash value with user's private key, as taught in Spies, with hash value disclosed in Trostle because encrypting a hash value with private key will further provide greater security against hackers and the user will be able to verify a document without any data compromise.

In claims 11,13,15, Trostle discloses computer storage and a server in (fig.1). Trostle discloses storage including respective IDs and encrypted private keys for the respective users in which private keys have been encrypted using respective keys determined from respective user identifying information and server reading an encrypted private key from the storage with corresponding to a particular user and transmitting the encrypted private key to the particular user in (fig.5 and col.5, lines 49-57). Trostle does not teach encrypting/decrypting hash value using

the user's private key. Spies discloses this features in (col.9, lines 15-30). It would have been obvious to person of ordinary skill in the art at the time the invention was made encrypt hash value with user's private key, as taught in Spies, with hash value disclosed in Trostle because encrypting a hash value with private key will further provide a grater security against hackers and the user will be able to verify a document without any data compromise.

6 Claims 2,6,12,14,16,19, are rejected under 35 U.S.C. 103(a) as being unpatentable over Trostle in view of Spies and further in view of Schneier.

In claims 2,6,12,19, Trostle discloses all the limitations above. However, Trostle does not discloses passphrase. Schneier discloses passphrase scheme in (page 174, passphrase section). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use passphrase taught in Schneier for password of Trostle so that user can remember phrases easier than random character sequences. Passphrase provides greater security through increased entropy than a short password. Trostle does not discloses destroying any non-volatile record of the private key at the location of the user. Trostle does discloses destroying a password at user's location in (col.6, lines 3-6). It would have been obvious to a person of ordinary skill in the art to modify the invention of Trostle to erase both private key and password because by completely deleting password as well as private key would greatly reduces chance of stealing valuable data by hackers thus providing greater security..

In claims 14,16 the examiner asserts that storage means the respective public keys corresponding to the private keys for the respective users is well known public key scheme. One

of ordinary skill in the art would be motivated to use public key method because it is much secure than secret key scheme.

In claim 19, see claim rejection 11 and 12 above.

Response to Amendment

7. Applicant has canceled claims 3,4,9,10,17-18, and amended claims 1,11,13-16. . See rejections above.

8. Applicant has corrected abstract and therefore objection to the abstract is withdrawn.

Conclusion

9 **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

10. Any inquiry concerning this communication should be directed to Ho S. Song at telephone number (703)305-0042. The examiner can normally be reached on Monday through Friday from 6:00 am to 4:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gail Hayes, can be reached at (703)305-9711.

Any inquiry of a general nature or relating to the status of this application or preceding should be directed to the group receptionist, whose telephone number is (703)305-3900.

Ho Song

Gail Hayes

GAIL HAYES
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100